

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-315036

(43)Date of publication of application : 08.11.1994

(51)Int.Cl.

H04L 12/54

H04L 12/58

G06F 13/00

G06F 15/21

H04L 9/32

(21)Application number : 05-102676

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 28.04.1993

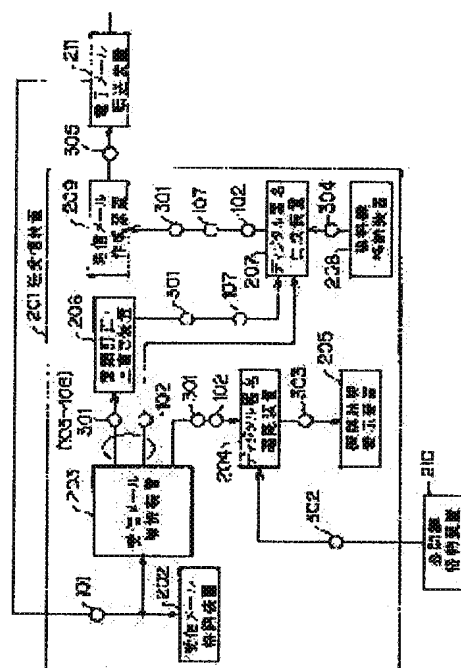
(72)Inventor : MOTOIKE SACHIKO

(54) ELECTRONIC MAIL SYSTEM WITH DIGITAL SIGNATURE

(57)Abstract:

PURPOSE: To receive a document described and signed by plural persons as electronic mail with digital signature, to confirm the priority and further to transmit it as the electronic mail with digital signature after being additionally signed.

CONSTITUTION: A signature information file 102 and plural entity files 103-106 are made into one piece of document data and defined as the target of transmission/reception, after the reception, the document is analyzed by a received mail analyzer 203, and the digital signature applied to the entity files is confirmed by a digital signature confirming device 204 by using a public key 302 of a signing persons. Further, a new entity file 107 is generated by copying the latest entity file, thereby the entity file is additionally described by a document correcting/overwriting device 206, and the digital signature is generated by a digital signature generator 207 by using a public key 304 of an additional describing person to all the entity files.



(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-315036

(43)公開日 平成6年(1994)11月8日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 12/54				
12/58				
G 0 6 F 13/00	3 5 1 G	7368-5B		
		8732-5K	H 0 4 L 11/ 20	1 0 1 B
		8949-5K	9/ 00	A
審査請求 未請求 請求項の数 3 O L (全 8 頁) 最終頁に続く				

(21)出願番号 特願平5-102676

(22)出願日 平成5年(1993)4月28日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 本 池 祥 子

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

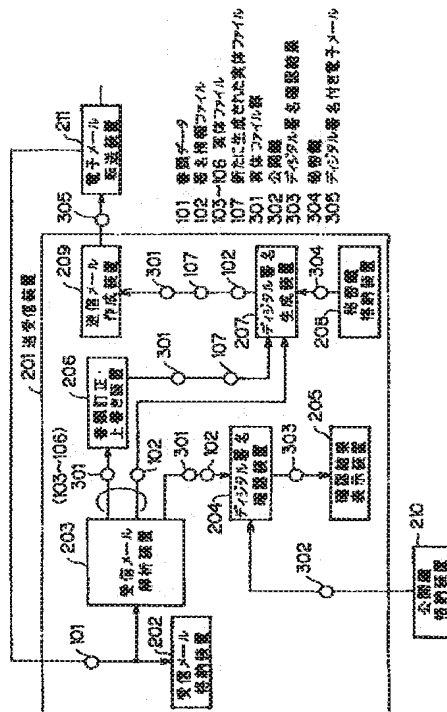
(74)代理人 弁理士 蔵合 正博

(54)【発明の名称】 デジタル署名付き電子メールシステム

(57)【要約】

【目的】 複数人によって記入され、署名された書類をデジタル署名付き電子メールとして受信し、その正当性を確認し、さらに追記して署名を施した上、デジタル署名付き電子メールとして送信できるようにする。

【構成】 署名情報ファイル102と複数の実体ファイル103~106を一つの書類データ101として送受信の対象とし、受信後に書類を受信メール解析装置203で解析して実体ファイルに施されたデジタル署名を署名者の公開鍵302を用いてデジタル署名確認装置204により確認する。さらに最新の実体ファイルをコピーして新たな実体ファイル107を生成し、追加記入はこの実体ファイルに対して書類訂正・上書き装置206で行ない、デジタル署名はすべての実体ファイルに対して追加記入者の秘密鍵304を用いてデジタル署名生成装置207により生成する。



【特許請求の範囲】

【請求項1】 複数ファイルをまとめて一つの電子メールとして取り扱うことが可能な電子メールシステムにおいて、電子メールを構成する複数ファイルのうちの一つを署名情報ファイルとし、残りを実体ファイルとし、署名情報ファイルには実体ファイル間に定義される論理的な依存関係とその依存関係に応じてそれぞれの実体ファイルに対して施されたデジタル署名の値とを記録して伝送する送受信装置を備えたデジタル署名付き電子メールシステム。

【請求項2】 送受信装置が、受信メールから署名情報ファイルと実体ファイルとを分離する受信メール解析手段と、前記受信メール解析手段から得られた実体ファイルと署名情報ファイルと署名者の公開鍵を用いて実体ファイルに施された複数人のデジタル署名の正当性を確認するデジタル署名確認手段とを備えた請求項1記載のデジタル署名付き電子メールシステム。

【請求項3】 送受信装置が、複数人のデジタル署名の施された受信メールに受信者が追加記入を行なって新たな実体ファイルを作成する訂正・上書き手段と、追加記入の加えられた受信メールと受信者の秘密鍵を用いて受信者のデジタル署名を生成するとともに、署名情報ファイルに実体ファイル間の論理構造とデジタル署名の値を記入するデジタル署名作成手段と、署名情報ファイルと実体ファイルとをまとめて送信メールを作成する送信メール作成手段とを備えた請求項2記載のデジタル署名付き電子メールシステム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、複数の利用者の間でデジタル署名を施した電子メールの送受信を行うデジタル署名付き電子メールシステムに関するものである。

【0002】

【従来の技術】従来、電子メールシステムでは、公開鍵暗号方式によるデジタル署名を施した電子メールが用いられている。以下、従来のこの種の電子メールシステムについて、図面を参照しながら説明する。

【0003】図5は従来のデジタル署名付き電子メールシステムの構成を示すものである。図5において、1はデジタル署名付き電子メールシステムのうち、送信用の電子メールにデジタル署名を施して送信する送信側装置であり、2は送信者の秘密鍵格納装置、3は送信メール作成装置、4はデジタル署名生成装置である。5はデジタル署名付き電子メールを転送する電子メール転送装置である。6は従来例におけるデジタル署名付き電子メールシステムのうち、電子メールを受信してデジタル署名の確認を行なう受信側装置であり、7は受信メール格納装置、8はデジタル署名確認装置、9はデジタル署名確認装置8の結果を受けてデジタル署名が正しいかどうかを表示する確認結果表示装置であ

る。10はデジタル署名を確認するのに必要な送信者の公開鍵を格納しておく、公開鍵格納装置である。

【0004】以上のように構成されたデジタル署名付き電子メールシステムにおいて、送信者Aが受信者Bに対してデジタル署名付きの電子メールを送付し、受信者Bが受け取った電子メールのデジタル署名を確認する場合の動作について説明する。

【0005】送信者Aが送信メール作成装置3を用いて受信者B宛の電子メール11を作成後、デジタル署名を付加して送信することを指示すると、電子メール11はデジタル署名生成装置4に送られる。デジタル署名生成装置4は、送信者Aの秘密鍵12を秘密鍵格納装置2から得て、電子メール11の内容からデジタル署名の値を計算し、それを電子メール11に付加したデジタル署名付き電子メール13を電子メール転送装置5に送る。これにより、送信者Aはデジタル署名付き電子メールを受信者B宛に送信することができる。

【0006】受信者B宛のデジタル署名付き電子メール13は、受信者Bの受信メール格納装置7に格納される。受信者Bがデジタル署名付き電子メール13の正当性の確認を指示すると、デジタル署名付き電子メール13は、デジタル署名確認装置8に送られる。デジタル署名確認装置8は、送信者Aの公開鍵14を公開鍵格納装置10から得て、デジタル署名付き電子メール13のデジタル署名の正当性を計算し、その結果を示すデータ15を確認結果表示装置9に送る。確認結果表示装置9は、データ15をもとに、正当性が確認されたか否かを受信者Bに表示する。

【0007】以上が、従来のデジタル署名付き電子メールシステムにおける送信者Aが受信者Bに対してデジタル署名付きの電子メールを送付し、受信者Bが受け取った電子メールのデジタル署名を確認する場合の動作である。

【0008】この方式は、送信者が複数の相手に対して同時にデジタル署名を施したメールを送信することを可能とし、さらにまた、署名付き電子メールをそのまま他の利用者に転送することで、元のメールの内容が正しく伝えられることを保証するものである。

【0009】

【発明が解決しようとする課題】しかしながら、上記従来の構成においては、決裁願や稟議書のように複数人が書き込みを行ないながら転送していく書類に対して、個々人が転送途中の同一書類への追加記入とデジタル署名を施しながら書類を送信することは、書類への追加記入そのものが、それまでの署名者のデジタル署名の正当性の確認を不可能とすることと等しい行為であることから、結果として電子メールにおけるデジタル署名の有効性を保持できないという問題点を有していた。

【0010】本発明は、上記従来の問題点を解決するもので、決裁願や稟議書のように複数人が書き込みを行な

い、かつ署名を施す書類であっても、デジタル署名の有効性を保持しながら電子メールによって転送することのできるデジタル署名付き電子メールシステムを提供することを目的とする。

【0011】

【課題を解決するための手段】上記目的を達成するために、本発明のデジタル署名付き電子メールシステムは、第一に、複数ファイルをまとめて一つの電子メールとして取り扱うことが可能な電子メールシステムにおいて、電子メールを構成する複数ファイルのうちの一つを署名情報ファイルとし、残りを実体ファイルとし、署名情報ファイルには、実体ファイル間に定義される論理的な依存関係とその依存関係に応じてそれぞれの実体ファイルに対して施されたデジタル署名の値とを記録して伝送する送受信装置を備えたものである。

【0012】また第二に、上記構成において、受信メールから署名情報ファイルと実体ファイルとを分離する受信メール解析手段と、受信メールを解析して得られた実体ファイルと署名情報ファイルと署名者の公開鍵を用いて実体ファイルに施された複数人のデジタル署名の正当性を確認するデジタル署名確認手段とを備えたものである。

【0013】また第三に、上記構成において、複数人のデジタル署名の施された受信メールに受信者が追加記入を行なって新たな実体ファイルを作成する訂正・上書き手段と、追加記入の加えられた受信メールと受信者の秘密鍵を用いて受信者のデジタル署名を生成するとともに、署名情報ファイルに実体ファイル間の論理構造とデジタル署名の値を記入するデジタル署名生成手段と、署名情報ファイルと実体ファイルとをまとめて送信メールを作成する送信メール作成手段とを備えたものである。

【0014】

【作用】本発明は、上記構成によって、複数ファイルを論理的に一つの書類と見なし、書類を構成する実体ファイルと、その実体ファイルが論理的に依存している他の実体ファイルに対してそれぞれの記入者のデジタル署名を施すことにより、決裁願や稟議書のように、複数人がそれぞれの場所を記入した上で捺印し、次の担当者に書類を回すような処理と同等の処理を、デジタル署名を用いて電子メールシステム上にて行なうことができる。

【0015】

【実施例】以下、本発明の一実施例について、図面を参照しながら説明する。図1は本発明の一実施例におけるデジタル署名付き電子メールシステムにおいて、送受信の対象とする書類のデータ構成を示す図である。図1において、101は書類データ全体を示し、102から106は書類データ101を構成する複数のファイルである。102は書類データ101の論理構造と、103

から106のそれぞれの実体ファイルに対して施されたデジタル署名の値を記録する署名情報ファイル、103から106は書類データ101の実体に相当する実体ファイルである。本図は実体ファイルが4つの場合を示しているが、その個数は一つ以上であればいくつでも良い。

【0016】図2は本発明の一実施例におけるデジタル署名付き電子メールシステムの装置構成を示す図である。図2において、201は本実施例のデジタル署名付き電子メールシステムのうち、特定の利用者ごとに必要となる送受信装置を示している。202は受信メール格納装置、203は受信メール解析装置、204はデジタル署名確認装置、205は確認結果表示装置、206は書類訂正・上書き装置、207はデジタル署名生成装置、208は秘密鍵格納装置、209は送信メール作成装置である。210は公開鍵格納装置、211は電子メール転送装置であり、これらはすべての利用者に共通の装置である。また、101、102はそれぞれ図1で示した書類データ、署名情報ファイルを示している。301は書類データ101を構成する実体ファイル群、107は追加記入により発生した新しい実体ファイル、302は署名情報ファイル102に記述されている署名の作成者の公開鍵、303はデジタル署名の確認結果を示すデータ、304は利用者の秘密鍵、305はデジタル署名付き電子メールである。

【0017】次に、上記装置における動作について説明するが、その前にまず、本実施例において送受信の対象となる書類の構成について、図1を用いて説明する。図1において、書類データ101は、複数のファイル102～106が論理的に一つの書類を構成しているファイル103から106までは、それぞれ利用者A、B、C、Dの作成した実体ファイルであり、それぞれの利用者の署名の値が、署名情報ファイル102に格納されている。CCITTのX.400に準拠したメールシステムにおいては、複数ファイルをまとめて送信するプロトコルが提供されているため、送信側・受信側とともに複数ファイルを論理的にまとめて一つとして扱うことができる。

【0018】実体ファイル103から実体ファイル106と、それぞれの利用者の署名の値との間には以下に示すような参照関係が存在する。

【0019】実体ファイル103は、利用者Aが作成したファイルであり、Aの署名は実体ファイル103のみに施されたもの、即ち実体ファイル103のみを用いてAの秘密鍵によって計算されたデジタル署名である。

【0020】これに対し、実体ファイル104は、実体ファイル103をコピーしたファイルに、利用者Bが追加記入や訂正を行なって作成したファイルであり、Bの署名は、これら二つの実体ファイル103と実体ファイル104とに施されたもの、即ち実体ファイル103と

5

実体ファイル104とを用いてBの秘密鍵によって計算されたデジタル署名である。

【0021】以下同様に、実体ファイル105は、実体ファイル104をコピーしたファイルに利用者Cが追加記入や訂正を行なったもの、実体ファイル106は、実体ファイル105をコピーしたファイルに利用者Dが追加記入や訂正を行なったものであり、また、Cの署名は、実体ファイル103から実体ファイル105までの三つのファイルに施されたもの、Dの署名は、実体ファイル103から実体ファイル106までの四つのファイルに施されたものである。

【0022】本実施例では、送受信の対象として、このような論理構造を持ったファイルの集まりを書類として利用する。

【0023】次に、図2を用いて書類データ101を受け取った利用者Eが書類の正当性を確認し、追加記入・修正を行ない、さらに次の利用者に書類を転送する方法を説明する。

【0024】利用者Eが電子メール転送装置31を介して利用者Dから受け取ったデジタル署名付き電子メールの書類データ101は、一旦受信メール格納装置202に格納され、書類データ101の正当性の確認を行なうために、受信メール解析装置203に送られる。受信メール解析装置203では、書類データ101を解析し、署名情報ファイル102と、四つの実体ファイル103、104、105、106からなる実体ファイル群301とをデジタル署名確認装置204に出力する。署名情報ファイル102には、図1を用いて説明したように、利用者Aから利用者Dのそれぞれの署名の値と各実体ファイルの間に存在する論理構造が記述されている。

【0025】デジタル署名確認装置204は、署名情報ファイル102に記述されている実体ファイル間の論理構造に従い、公開鍵格納装置200から利用者Aから利用者Dのそれぞれの公開鍵302を得て、以下のような順序で署名の正当性の確認を行ない、その結果を送受信装置201内の図示されないメモリに記憶しておく。

【0026】まず、実体ファイル103の正当性を、署名情報ファイル102に記述されているAの署名の値と公開鍵格納装置210からのAの公開鍵を用いて確認する。これにより、書類データ101を構成する実体ファイルのうち、もともと利用者Aが作成した実体ファイル103の正当性を確認することができる。

【0027】次に、実体ファイル104の正当性を、署名情報ファイル102に記述されているBの署名の値と実体ファイル103とBの公開鍵を用いて確認する。Bの署名の値は、実体ファイル103、104の双方を用いて計算されているためである。これにより、書類データ101を構成する実体ファイルのうち、利用者Bは利用者Aの作成した実体ファイル103を用いて実体フ

6

イル104を作成し、署名したことが確認でき、実体ファイル104自身の正当性と、実体ファイル103と104との依存関係についての正当性を確認することができる。

【0028】以下同様に、実体ファイル105、106それぞれの正当性と、実体ファイル103から105の依存関係、実体ファイル103から106の依存関係についての正当性を順次確認することができ、最終的に、全体として書類データ101が利用者Aから利用者Dによって順次正当に作成されたものであることを確認することができる。確認結果を示すデータ303は確認結果表示装置25に送られ、利用者Eは署名の正当性を確認することができる。

【0029】さて、利用者Eがこのような書類データ101に対して、追加記入の開始を指示すると、書類訂正・上書き装置206は、実体ファイル群301を得て、最新の实体ファイルである106をコピーし、利用者Eに対して追加記入可能な状態とする。利用者Eがこれに対して追加記入を行ない、追加記入の終了を指示すると、利用者Eによって新しく作成された実体ファイル107と実体ファイル群301、署名情報ファイル102は、デジタル署名生成装置207に送られる。デジタル署名生成装置207は、実体ファイル群301と実体ファイル107に対して、秘密鍵格納装置208から得た利用者Eの秘密鍵304を用いて署名の値を計算し、その結果を署名情報ファイル102に書き込み、また、実体ファイル103から107の間に存在する論理構造をも同時に書き込む。

【0030】最終的に、送信メール作成装置209は、署名情報ファイル102と、実体ファイル103から107によって構成される送信メール305を形成し、電子メール転送装置211に送信メールを渡す。

【0031】このようにして、利用者Eは、書類データ101の正当性を確認することができ、また、さらに追加記入の上、利用者E自身の署名を施し、他の利用者にデジタル署名付き電子メールとして送信することができる。

【0032】図3および図4は上記実施例の動作より具体的に示したものである。図3において、100は書類データ101を従来形式の書類としてイメージ化したもので、ここでは決裁願を例にしている。いま、起案者A（松下）が、ワークステーション3台の購入を申請するために決裁願を起案したものとする。これを電子メールにより上司の係長に転送する場合、申請内容を表わした実体ファイル103と、実体ファイル103を基に計算された起案者Aの印鑑に相当する署名の値および実体ファイル間の論理構造（この場合はファイルがひとつなので、自身のファイル名）が記述された署名情報ファイル102とからなる書類データ101が作成される。

【0033】図4において、このような書類データに基

づく電子メールを係長が起案者Aから受信すると、係長はこれを受信メール解析装置203により実体ファイル103と署名情報ファイル102とに分離して、デジタル署名確認装置204により署名の有効性を確認するとともに、内容を確認して、ワークステーション3台は無理なので、これを書類訂正・上書き装置206により2台に訂正して、実体ファイル103を基にして新たな実体ファイル104を生成するとともに、デジタル署名生成装置207により署名情報ファイル102に実体ファイル103と104を基に計算された係長（木村）の署名の値と実体ファイル間の論理構造（この場合は実体ファイル103と104との関係）を追加記述して送信メールを作成し、次の課長宛に電子メールで送信する。

【0034】このようにして受信者が順次実体ファイルを作成し、署名情報ファイルにその署名の値および新たに作成された実体ファイル間の論理構造を追加記述した書類データを作成することにより、最終の決裁者は、起案者以降のすべての実体ファイルの内容および署名を確認することができ、最終判断を的確に行なうための情報を得ることができる。

【0035】

【発明の効果】以上のように本発明は、実体ファイルと署名情報ファイルから構成される書類データを解析し、署名の正当性を確認するとともに、新たな実体ファイルを追加して、それへの署名を生成して追加記入することにより、複数人によって記入され、また署名された書類をデジタル署名の有効性を保持しながら署名付き電子メールとして送受信することができる。

【図面の簡単な説明】

【図1】本発明の一実施例におけるデジタル署名付き電子メールシステムにおいて送受信の対象とする書類デ

ータのデータ構成図

【図2】本発明の一実施例におけるデジタル署名付き電子メールシステムの送受信装置の構成を示すブロック図

【図3】本発明の一実施例におけるデジタル署名付き電子メールシステムの動作を示す模式図

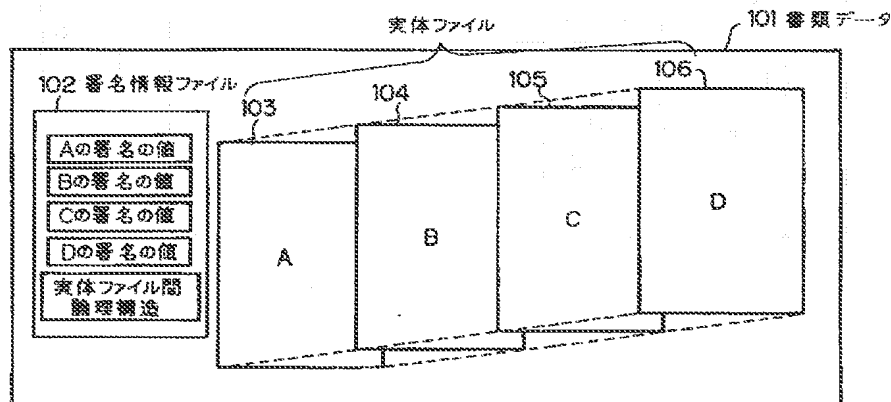
【図4】本発明の一実施例におけるデジタル署名付き電子メールシステムの動作を示す模式図

【図5】従来例におけるデジタル署名付き電子メールシステムのシステム構成図

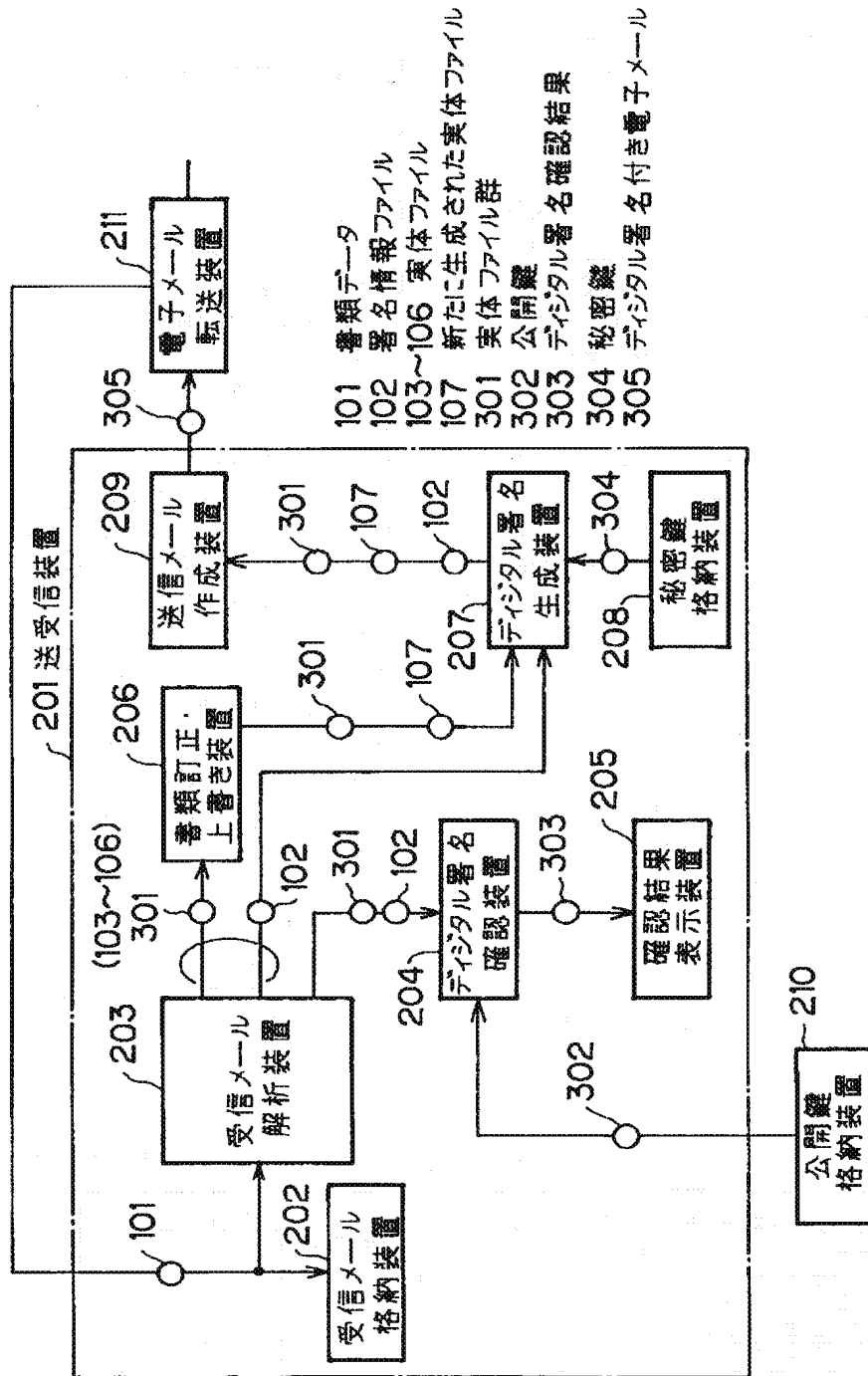
【符号の説明】

- 100 従来形式の書類
- 101 書類
- 102 署名情報ファイル
- 103～107 実体ファイル
- 201 送受信装置
- 202 受信メール格納装置
- 203 受信メール解析装置
- 204 デジタル署名確認装置
- 205 確認結果表示装置
- 206 書類訂正・上書き装置
- 207 デジタル署名生成装置
- 208 秘密鍵格納装置
- 209 送信メール作成装置
- 210 公開鍵格納装置
- 211 電子メール転送装置
- 301 実体ファイル群
- 302 公開鍵群
- 303 デジタル署名確認結果
- 304 秘密鍵
- 305 デジタル署名付き電子メール

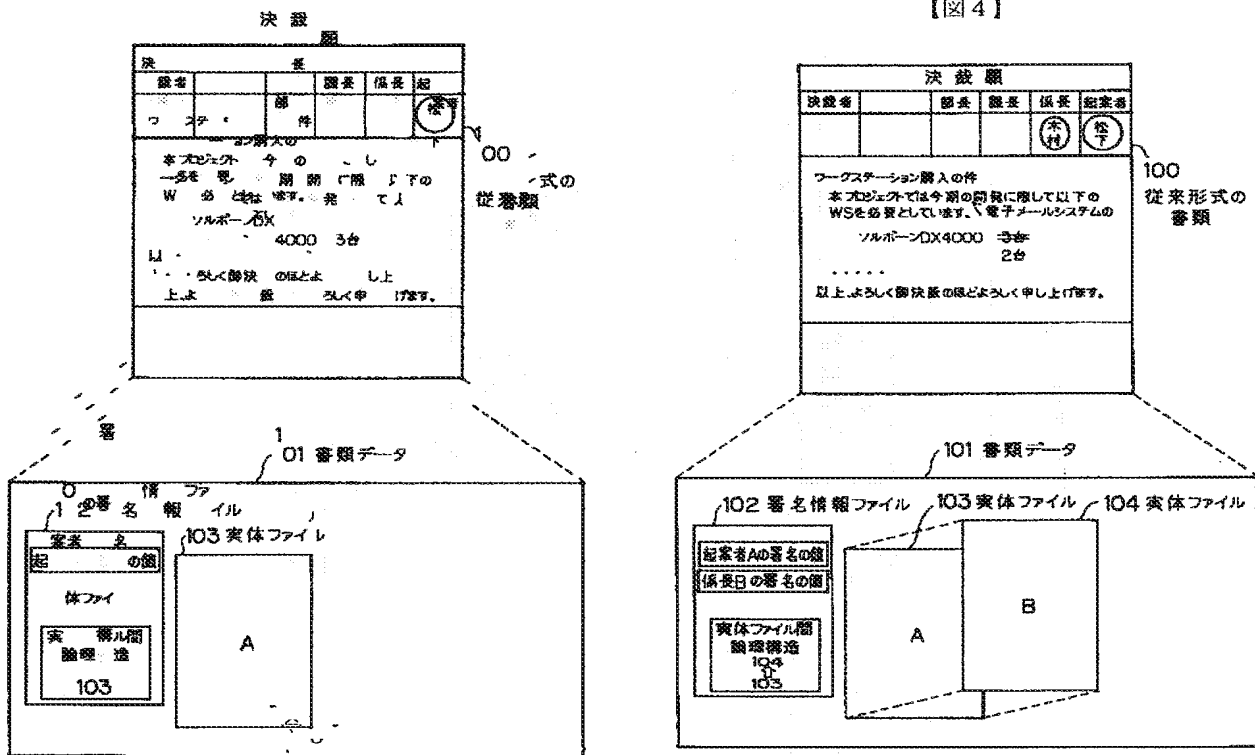
【図1】



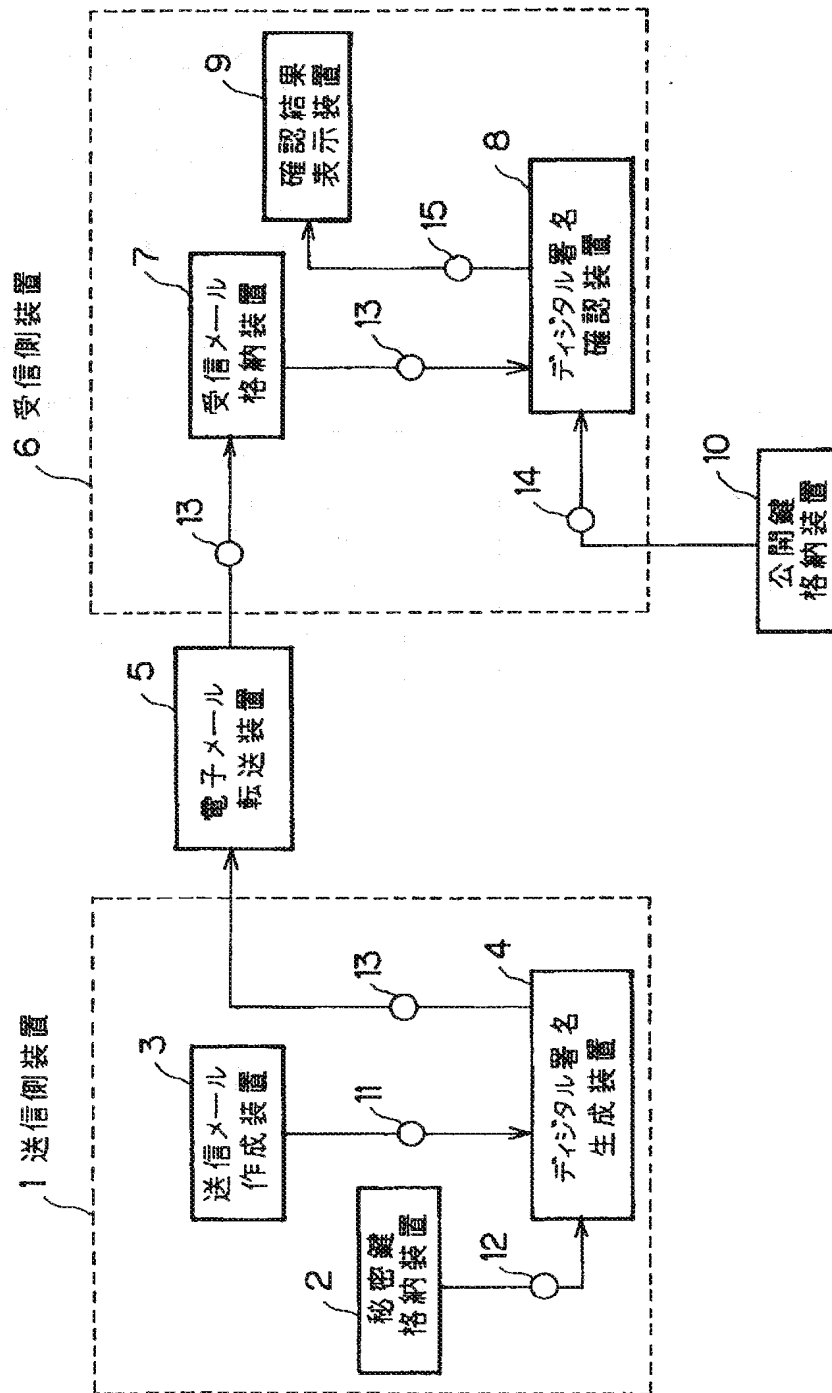
【図2】



【図4】



【図5】



フロントページの続き

(51) Int. Cl. 5

G 0 6 F 15/21

H 0 4 L 9/32

識別記号 庁内整理番号

3 4 0 B 8724-5L

F I

技術表示箇所